TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
SP16207.C RS		
Demande internationale n°	Date du dépôt international *(jour/mois/année)*	(Date de priorité (la plus ancienne) *(jour/mois/année)*
PCT/FR 00/ 00174	26/01/2000	27/01/1999
Déposant		
FRANCE TELECOM et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

   a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

   [ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

   b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

   [ ] contenu dans la demande internationale, sous forme écrite.

   [ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

   [ ] remis ultérieurement à l'administration, sous forme écrite.

   [ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   [ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   [ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre**,

   [X] le texte est approuvé tel qu'il a été remis par le déposant.

   [ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne **l'abrégé**,

   [X] le texte est approuvé tel qu'il a été remis par le déposant

   [ ] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure des dessins à publier avec l'abrégé est la Figure n°

   [ ] suggérée par le déposant.

   [ ] parce que le déposant n'a pas suggéré de figure.

   [ ] parce que cette figure caractérise mieux l'invention.

   [X] Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PC[illegible] 00/00174

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	BRANDT J ET AL: "Zero-knowledge authentication scheme with secret key exchange" ADVANCES IN CRYPTOLOGY - CRYPTO '88. PROCEEDINGS, SANTA BARBARA, CA, USA, 21-25 AUG. 1988, pages 583-588, XP000090662 1990, Berlin, West Germany, Springer-Verlag, West Germany ISBN: 3-540-97196-3 page 584, alinéa 4 --- -/--	1,6

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
18 février 2000	25/02/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Zucka, G

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 00/00174

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	FIAT A ET AL: "How to prove yourself: practical solutions to identification and signature problems" ADVANCES IN CRYPTOLOGY - CRYPTO '86 PROCEEDINGS, SANTA BARBARA, CA, USA, 11-15 AUG. 1986, pages 186-194, XP000090668 1987, Berlin, West Germany, Springer-Verlag, West Germany ISBN: 3-540-18047-8 cité dans la demande page 187 -page 188	1,6
A	KONIGS H -P: "Cryptographic identification methods for smart cards in the process of standardization" IEEE COMMUNICATIONS MAGAZINE, JUNE 1991, USA, vol. 29, no. 6, pages 42-48, XP002126721 ISSN: 0163-6804 page 46, colonne 2 -page 47, colonne 2	1-7
A	GUILLOU L C ET AL: "A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory" ADVANCES IN CRYPTOLOGY - EUROCRYPT '88. WORKSHOP ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. PROCEEDINGS, DAVOS, SWITZERLAND, 25-27 MAY 1988, pages 123-128, XP000562467 1988, Berlin, West Germany, Springer-Verlag, West Germany ISBN: 3-540-50251-3 cité dans la demande page 125 -page 127	1,6
A	QUISQUATER J -J ET AL: "Fast decipherment algorithm for RSA public-key cryptosystem" ELECTRONICS LETTERS, 14 OCT. 1982, UK, vol. 18, no. 21, pages 905-907, XP000577331 ISSN: 0013-5194 cité dans la demande figure 1	5
A	FR 2 752 122 A (FRANCE TELECOM) 6 février 1998 (1998-02-06) cité dans la demande page 6 -page 13	1-7
A	FR 2 716 058 A (FRANCE TELECOM ;POSTE) 11 août 1995 (1995-08-11) cité dans la demande page 8 -page 13, alinéa 2	1-7

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
FR 00/00174

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
FR 2752122	A	06-02-1998	AUCUN		
FR 2716058	A	11-08-1995	DE	69505703 D	10-12-1998
			DE	69505703 T	02-06-1999
			EP	0666664 A	09-08-1995

Translation

689557

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference SP16207.C RS	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR00/00174	International filing date (*day/month/year*) 26 January 2000 (26.01.00)	Priority date (*day/month/year*) 27 January 1999 (27.01.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/32		
Applicant	FRANCE TELECOM	

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 6 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
22 July 2000 (22.07.00)	19 December 2000 (19.12.2000)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR00/00174

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1-4,8-12, as originally filed,
pages _____, filed with the demand,
pages 5-7, filed with the letter of 02 October 2000 (02.10.2000).
pages _____, filed with the letter of _____.

☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-7, filed with the letter of 02 October 2000 (02.10.2000).
Nos. _____, filed with the letter of _____.

☐ the drawings, sheets/fig _____, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-7	YES
	Claims		NO
Inventive step (IS)	Claims	1-7	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-7	YES
	Claims		NO

2. Citations and explanations

1. Reference is made to the following documents:

D1: Brandt, J. et al.: 'Zero-knowledge authentication scheme with secret key Exchange' Advances in Cryptology - Crypto '88 Proceedings, Santa Barbara, CA, USA, 21-25 AUG. 1988, pages 583-588, XP000090662 1990, Berlin, West Germany, Springer-Verlag, ISBN: 3-540-97196-3

2. Document D1, which is cited on page 5 of the amended description, discloses (see, in particular, page 584, paragraph 4) an authentication method using a first entity to be authenticated (P), having a public key **e** and a secret key **d**, said keys being connected by a modulus **n** operation, and a second, authenticating entity (V) to which public key **e** is known, said entities having information exchanging means requiring zero knowledge transfer ("zero-knowledge interactive proof system") and being capable of performing cryptographic calculations in connection with said information, wherein some of the calculations are performed with modulus **n**.

Each entity to be authenticated has its own modulus

n, and it is obvious to a person skilled in the art that said modulus must necessarily be communicated in some way to the authenticating entity.

However, D1 does not disclose the feature whereby the modulus **n** operation is $v = s^{-t} \bmod n$, where t is a parameter. Therefore, the subject matter of independent claims 1 and 6 is novel.

3. Said feature is advantageous in that it reduces the number of calculations performed by the authenticated entity by a factor of up to 2 or 3.

None of the documents cited in the search report discloses such a procedure or renders it obvious. Therefore, an inventive step is acknowledged.

4. It follows that the subject matter of dependent claims 2-5 and 7 is also novel and inventive.

5. The subject matter of claims 1-7 is industrially applicable.

5T

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire SP16207.C RS	**POUR SUITE A DONNER** voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR00/00174	Date du dépot international *(jour/mois/année)* 26/01/2000	Date de priorité *(jour/mois/année)* 27/01/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/32		
Déposant FRANCE TELECOM et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.

   ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent 6 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

   - I ☒ Base du rapport
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☐ Irrégularités dans la demande internationale
   - VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 22/07/2000	Date d'achèvement du présent rapport 19.12.2000
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tél. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Fonctionnaire autorisé Zucka, G N° de téléphone +31 70 340 4026

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/00174

I. Base du rapport

1. Ce rapport a été rédigé sur la base des éléments ci-après (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17).*) :

Description, pages:

1-4,8-12	version initiale			
5-7	reçue(s) le	02/10/2000	avec la lettre du	28/09/2000

Revendications, N°:

1-7	reçue(s) le	02/10/2000	avec la lettre du	28/09/2000

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.
   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
   ☐ remis ultérieurement à l'administration, sous forme écrite.
   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

   ☐ de la description, pages :

☐ des revendications, n^{os} :

☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-7
	Non :	Revendications	
Activité inventive	Oui :	Revendications	1-7
	Non :	Revendications	
Possibilité d'application industrielle	Oui :	Revendications	1-7
	Non :	Revendications	

2. Citations et explications
   voir feuille séparée

Les dispositions de l'article 34(2) b) PCT ont été satisfaites; la caractéristique ajoutée aux revendications indépendantes vient de la revendication 2 initiale.

Concernant le point V

1. Il est fait référence au document suivant:

   D1 = Brandt J. et al.: 'Zero-knowledge authentication scheme with secret key Exchange' Advances in Cryptology - Crypto '88 Proceedings, Santa Barbara, CA, USA, 21-25 AUG. 1988, pages 583-588, XP000090662 1990, Berlin, West Germany, Springer-Verlag, ISBN: 3-540-97196-3

2. Le document D1, qui est cité à la page 5 de la description modifiée, divulgue (voir surtout la page 584, paragraphe 4) un procédé d'authentification mettant en oeuvre une première entité à authentifier (P), possédant une clé publique **e** et une clé secrète **d**, ces clés étant reliées par une opération modulo **n**, et une seconde entité authentifiante (V), connaissant la clé publique **e**, ces entités, comprenant des moyens aptes à échanger des informations du type à apport nul de connaissance ("zero-knowledge interactive proof system") et à effectuer des calculs cryptographiques portant sur ces informations, certains calculs étant effectués modulo **n**.

   Chaque entité à authentifier possède sa propre module **n**, et il est clair pour l'homme du métier que cette module doit nécessairement être communiquée d'une manière ou d'une autre à l'entité authentifiante.

   D1 ne divulgue cependant pas la caractéristique selon laquelle l'opération modulo **n** est du type $v=s^{-t} \bmod n$, t étant un paramètre. L'objet des revendications indépendantes 1 et 6 est par conséquent nouveau.

3. Ladite caractéristique a comme avantage de réduire le nombre de calculs effectués par l'entité authentifiée, jusqu'à un facteur de 2 ou 3.

   Aucun document cité dans le rapport de recherche ne divulgue ou ne rend évident

une telle manière de procéder, et l'activité inventive est par conséquent reconnue.

4. L'objet des revendications dépendantes 2-5 et 7 est donc également nouveau et inventif.

5. L'objet des revendications 1-7 est susceptible d'une application industrielle.

dire généré par une tierce partie de confiance, mémorisé et utilisé par toutes les entités qui y sont rattachées. Le caractère universel de n implique qu'il est de très grande taille (typiquement 1024 bits), car la découverte de la factorisation de n compromettrait les clés secrètes de tous les utilisateurs.

Dans leur version de base, aucun des protocoles mentionnés plus haut ne peut être mis en oeuvre dans une application soumise à de fortes contraintes, (bas coût, faible complexité) telles que décrites dans la section précédente, car les calculs requis ne pourraient être effectués par une carte à microcircuit qui ne serait pas dotée d'un cryptoprocesseur.

La demande de brevet français FR-A-2 752 122 décrit bien une optimisation de ces protocoles, mais cette optimisation reste limitée aux protocoles basés sur le logarithme discret dans un mode dit "à précalculs" qui présente l'inconvénient d'impliquer des rechargements à intervalles réguliers.

Le document J. BRANDT et al. intitulé "Zero-knowledge Authentication Scheme with Secret Key Exchange" publié dans Advances in Cryptology-Crypto 88 Proceedings, XP 000090662, pages 583-588, décrit un schéma d'authentification sans apport de connaissance, avec échange de clé secrète entre deux utilisateurs, schéma dans lequel l'entité à authentifier calcule son propre module n=pq et met en oeuvre une opération du type $m^d \pmod n$.

La présente invention vise à réduire le nombre de calculs effectués par l'entité authentifiée dans les protocoles d'identification (ou d'authentification de message ou de signature de message) sans apport de connaissance basés sur la factorisation, cette réduction

pouvant atteindre un facteur 2 ou 3 dans le cadre d'une opération particulière du type $v=s^{-t} \pmod n$.

Elle rend ainsi possible, et plus particulièrement quand on la couple avec le protocole Guillou-Quisquater, l'exécution rapide d'un algorithme d'identification (ou d'authentification de message ou de signature de message) à clé publique dans une carte à microcircuit standard à bas coût, pour des applications telles que le porte-monnaie électronique ou la télécarte de future génération.

Exposé de l'invention

Le module n étant un paramètre de type individuel (en d'autres termes, chaque utilisateur possède sa propre valeur de n), on peut exploiter ce choix des deux manières suivantes, (qui peuvent d'ailleurs être avantageusement combinées) :

1) d'abord en choisissant une taille de n inférieure à la valeur usuelle (typiquement inférieure à 1000 et par exemple comprise entre 700 et 800) ; cela est possible car la découverte de la factorisation de n ne compromet plus que la clé secrète de l'utilisateur correspondant et en aucune façon celle des autres ; cette seule modification permet de réduire déjà d'environ 40% la durée des calculs effectués modulo n ;
2) si l'utilisateur a conservé les facteurs premiers de n dans la mémoire de son dispositif de sécurité, on peut mettre en oeuvre la technique dite des restes chinois, pour réduire encore d'environ 40% la durée des calculs effectués modulo n, lorsque le nombre de facteurs premiers est 2 ; cette réduction peut être encore amplifiée en utilisant plusieurs facteurs premiers (typiquement 3 ou 4).

Au total, on peut donc réduire les temps de calcul modulo n d'au moins 60%, c'est-à-dire d'au moins un facteur 2.

De façon précise, l'invention a pour objet un procédé d'authentification mettant en oeuvre une première entité dite "à authentifier", possédant une clé publique $\underline{v}$ et une clé secrète $\underline{s}$, ces clés étant reliées par une opération modulo $\underline{n}$ où $\underline{n}$ est un entier appelé module qui est propre à l'entité à authentifier, et une seconde entité dite "authentifiante", connaissant la clé publique $\underline{v}$, ces entités comprenant des moyens aptes à échanger des informations du type à apport nul de connaissance et à effectuer des calculs cryptographiques portant sur ces informations, certains calculs étant effectués modulo $\underline{n}$, ce procédé étant caractérisé en ce que le module l'opération modulo n est du type $v=s^{-t} \pmod n$, t étant un paramètre.

Les entités dont il est question peuvent être, par exemple des cartes à microcircuit, des porte-monnaie électroniques, des télécartes, etc ...

Dans un mode de mise en oeuvre avantageux, les échanges d'informations du type à apport nul de connaissance et les calculs cryptographiques sont les suivants :

- l'entité à authentifier choisit au hasard un (des) nombre(s) entier(s) $\underline{r}$ compris entre 1 et n-1 et calcule un (des) paramètre(s) $\underline{x}$ égal (égaux) à $r^t \pmod n$, puis un (des) nombre(s) $\underline{c}$ appelé(s) engagement(s) qui est (sont) une (des) fonction(s) de ce (ces) paramètre(s) et éventuellement d'un message (M), et envoie cet (ces) engagement(s) à l'entité authentifiante ;
- l'entité authentifiante reçoit le ou les engagement(s) $\underline{c}$, choisit au hasard un nombre $\underline{e}$

REVENDICATIONS

1. Procédé d'authentification mettant en oeuvre une première entité dite "à authentifier" (A), possédant une clé publique $\underline{v}$ et une clé secrète $\underline{s}$, ces clés étant reliées par une opération modulo $\underline{n}$ où $\underline{n}$ est un entier appelé module, le module $\underline{n}$ étant propre à l'entité à authentifier (A), et une seconde entité dite "authentifiante" (B), connaissant la clé publique $\underline{v}$, ces entités, comprenant des moyens aptes à échanger des informations du type à apport nul de connaissance et à effectuer des calculs cryptographiques portant sur ces informations, certains calculs étant effectués modulo $\underline{n}$, ce procédé étant caractérisé en ce que l'opération modulo $\underline{n}$ est du type $v=s^{-t} \pmod n$, t étant un paramètre.

2. Procédé selon la revendication 1, dans lequel les échanges d'informations du type à apport nul de connaissance et les calculs cryptographiques sont les suivants :

- l'entité à authentifier (A) choisit au hasard un (des) nombre(s) entier(s) $\underline{r}$ compris entre 1 et n-1 et calcule un (des) paramètre(s) (x) égal (égaux) à $r^t \pmod n$, puis un (des) nombre(s) $\underline{c}$ appelé(s) engagement(s) qui est (sont) une (des) fonction(s) de ce (ces) paramètre(s) et éventuellement d'un message (M), et envoie cet (ces) engagement(s) à l'entité authentifiante (B) ;

- l'entité authentifiante (B) reçoit le ou les engagement(s) c, choisit au hasard un nombre e appelé "question" et envoie cette question à l'entité à authentifier (A) ;
- l'entité à authentifier (A) reçoit la question e, effectue un (des) calcul(s) utilisant cette question e et la clé secrète s, le résultat de ce (ces) calcul(s) constituant une (des) réponse(s) y, et envoie cette (ces) réponse(s) à l'entité authentifiante (B) ;
- l'entité authentifiante (B) reçoit la (les) réponse(s) y, effectue un calcul utilisant la clé publique v et le module n, et vérifie par une opération modulo n que le résultat de ce calcul est bien cohérent avec le (les) engagement(s) reçu(s).

3. Procédé selon la revendication 2, dans lequel la taille du nombre n, exprimée en nombre de bits, est inférieure à 1 000.

4. Procédé selon la revendication 3, dans lequel la taille du nombre n est comprise entre 700 et 800.

5. Procédé selon l'une quelconque des revendications 1 à 4, dans lequel n est le produit d'au moins deux nombres premiers (p, q) et dans lequel les opérations modulo n sont effectuées par la méthode dite "des restes chinois".

6. Procédé de signature de message par une entité dite "signataire" (A), cette entité possédant une clé publique $\underline{v}$ et une clé secrète $\underline{s}$, ces clés étant reliées par une opération modulo n où $\underline{n}$ est un entier appelé "module" qui est propre au signataire, comprenant des moyens aptes à calculer un engagement $\underline{c}$ fonction notamment du message à signer M et un nombre $\underline{y}$ fonction de la clé secrète, à émettre les nombres $\underline{y}$ et $\underline{c}$ qui constituent la signature du message M et le message M, ce procédé étant caractérisé en ce que l'opération modulo n est l'opération $v=s^{-t} \pmod{n}$, t étant un paramètre.

7. Procédé de signature selon la revendication 6, dans lequel le signataire choisit au hasard un nombre entier $\underline{r}$ compris entre 1 et n-1, calcule un paramètre $\underline{x}$ égal à $r^t \pmod{n}$, calcule un nombre $\underline{c}$ fonction du paramètre $\underline{x}$ et du message à signer M, calcule un nombre $\underline{y}$ à l'aide de sa clé secrète $\underline{s}$ et fonction des nombres $\underline{r}$ et $\underline{e}$, et émet les nombres $\underline{c}$ et $\underline{y}$ comme signature.

THE FOLLOWING IS THE ENGLISH TRANSLATION OF THE ANNEXES TO THE INTERNATIONAL PRELIMINARY EXAMINATION REPORT: AMENDED SHEETS (Pages 5, 6, 7, 13, 14 and 15).

In their basic versions, none of the above mentioned protocols can be implemented in an application that has to comply with severe specifications (low cost, low sophistication), as described in the previous section, as the required calculations could not be performed by a microprocessor card without a cryptoprocessor.

Though the French patent application FR-A- 2 752 122 describes an optimisation of these protocols, it is restricted to protocols involving the discrete logarithm method following a mode called "with pre-calculations" that has the drawback of implying regularly scheduled reloads.

The present invention appropriately suppresses this drawback. It aims to reduce the number of calculations to be carried out by the prover when using zero-knowledge identification (or message signature or authentication) protocols involving factoring, the gain being liable to reach a factor 2 or 3.

It also enables - and in particular when coupled with the GUILLOU-QUISQUATER protocol - the fast completion of a public key identification (or message authentication or signature) algorithm included in a low cost standard microcircuit card, for applications such as the electronic purse or next generation telecard.

Description of the invention

This aim is fulfilled by selecting a modulus n which is not a universal value but an individual value (in other words, each entity has its own n value), and by using this selection in the following two ways (which may be advantageously combined):

1) first by retaining a length of n lower than the currently used values (typically lower than 1000 bits and for example, ranging between 700 and 800 bits); this is possible as breaking the factoring of n only compromises the secret key of the related user and in no way the secret keys of other users; this modification alone reduces the duration of calculations carried out modulo n by 40%;

2) If the user has stored the prime factors of n in the memory of his security device, he (or she) may use the Chinese remainders technique to reduce the duration of modulo n calculations by a further 40%, when there are two prime factors; this reduction may be increased when using several prime factors (typically 3 or 4).

On the whole, the modulo n calculations can then be reduced by 60%, that is a factor 2, at least.

Precisely, the invention relates to a process of identification involving a first entity called a "prover", which possesses a public key v and a secret key s, these keys being related by a modulo n calculation where n is an integer called modulus, and a second entity called a "verifier", which knows the

public key v, these entities being provided with means to exchange information in a zero-knowledge context and to carry out cryptographic calculations on this information, some calculations being performed in modulo n mode, the process being characterised by the fact that the value of n is specific to the prover entity, which communicates it to the verifier entity.

The aforementioned entities may be, for example, microcircuit cards, electronic purses, telecards, and so on...

Following a preferred implementation, the modulo n calculation is of the kind $v=s^{-t} \pmod n$, where t is a parameter and the zero-knowledge information exchanges are the following:

- the prover selects one (several) integer(s) at random, r ranging between 1 and n-1, and calculates one (several) parameter(s) x equal to $r^t \pmod n$, then one (several) number(s) c called opening(s) which is (are) one (several) function(s) of this (these) parameter(s) and possibly of a message (M), and sends this (these) opening(s) to the verifier;
- the verifier entity receives the opening(s) c, selects one number e called a "question" at random and sends this question to the prover ;
- the prover receives the question e, carries out one (several) calculation(s) using this question e and the secret key s, the result of this (these) calculation(s) yielding one

Claims

1. Authentication process involving a first entity called a "prover" (A), which possesses a public key $\underline{v}$ and a secret key $\underline{s}$, these keys being related by an operation modulo $\underline{n}$, where $\underline{n}$ is an integer called modulus, and a second entity called a "verifier" (B), which knows the public key $\underline{v}$, wherein these entities are provided with means to exchange zero-knowledge information and carry out cryptographic calculations on this information, some calculations being carried out modulo $\underline{n}$, the process being characterised in that the modulus $\underline{n}$ is specific to the prover (A), which communicates this modulus to the verifier (B).

2. Process according to claim 1, wherein the modulo $\underline{n}$ calculation is of the type $v=s^{-t} \pmod n$, t being a parameter, wherein the information exchanges are of zero-knowledge type and wherein the cryptographic calculations are completed as follows:

- the prover (A) selects one (several) integer(s) $\underline{r}$ at random, ranging between 1 and n-1 and calculates one (several) parameter(s) (x) equal to $r^t \pmod n$, then one (several) number(s) $\underline{c}$ called opening(s) which is (are) one (several) function(s) of this (these) parameter(s) and possibly of a message (M), and sends this (these) opening(s) to the verifier (B);
- the verifier entity (B) receives the opening(s) $\underline{c}$, selects one number e at

random called "question" and sends this question to the prover (A);

- the prover (A) receives the question e, carries out one (several) calculation(s) using this question e and the secret key s, the result of this (these) calculation(s) yielding one (several) answer(s) y and sends this (these) answer(s) to the verifier (B).
- The verifier (B) receives the answer(s) y, carries out one calculation using the public key v and the modulus n, and checks with a modulo n calculation that the result is coherent with the received opening(s).

3. Process according to claim 2, wherein the size of the number n, expressed in number of bits, is less than 1 000.

4. Process according to claim 3, wherein the size of the number n is between 700 and 800.

5. Process according to any of claims 1 to 4, wherein n is the product of at least two primes (p and q) and wherein the modulo n calculations are performed according to the method called "Chinese remainders".

6. Message signature process intended for a signatory (A) provided with a public key v and a secret key s, wherein these keys are related via a modulo n calculation, where n is an integer called modulus, the

said process involving means to calculate an opening $\underline{c}$ that is notably function of the message M to be signed, able to calculate a number $\underline{y}$ that is a function of the secret key, and able to transmit the numbers $\underline{y}$ and $\underline{c}$ that are the signature of the message and to transmit the message M, the process being characterised in that the modulus n is specific to the signatory.

7. Signature process according to claim 6, wherein the modulo n operation is the relation $v=s^{-t} \pmod n$ and wherein the signatory selects an integer $\underline{r}$ at random between 1 and n-1, calculates a parameter $\underline{x}$ equal to $r^t \pmod n$, calculates a number $\underline{c}$ that is a function of parameter $\underline{x}$ and message M to be signed, calculates a number $\underline{y}$ using its secret key $\underline{s}$, the said number $\underline{y}$ being a function of numbers $\underline{r}$ and $\underline{e}$, and transmits the numbers $\underline{c}$ and $\underline{y}$ as signature.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur : le BUREAU INTERNATIONAL

PCT

NOTIFICATION RELATIVE A LA PRESENTATION OU A LA TRANSMISSION DU DOCUMENT DE PRIORITE

(instruction administrative 411 du PCT)

Destinataire:

DU BOISBAUDRY, Dominique
Société De Protection Des Inventions
3, Rue Du Docteur Lancereaux
F-75008 Paris
FRANCE

Date d'expédition (jour/mois/année) 15 février 2000 (15.02.00)	
Référence du dossier du déposant ou du mandataire SP16207.C RS	**NOTIFICATION IMPORTANTE**
Demande internationale no PCT/FR00/00174	Date du dépôt international (jour/mois/année) 26 janvier 2000 (26.01.00)
Date de publication internationale (jour/mois/année) Pas encore publiée	Date de priorité (jour/mois/année) 27 janvier 1999 (27.01.99)
Déposant FRANCE TELECOM etc	

1. La date de réception (sauf lorsque les lettres "NR" figurent dans la colonne de droite) par le Bureau international du ou des documents de priorité correspondant à la ou aux demandes énumérées ci-après est notifiée au déposant. Sauf indication contraire consistant en un astérisque figurant à côté d'une date de réception, ou les lettres "NR", dans la colonne de droite, le document de priorité en question a été présenté ou transmis au Bureau international d'une manière conforme à la règle 17.1.a) ou b).
2. Ce formulaire met à jour et remplace toute notification relative à la présentation ou à la transmission du document de priorité qui a été envoyée précédemment.
3. Un **astérisque(*)** figurant à côté d'une date de réception dans la colonne de droite signale un document de priorité présenté ou transmis au Bureau international mais de manière non conforme à la règle 17.1.a) ou b). Dans ce cas, **l'attention du déposant est appelée** sur la règle 17.1.c) qui stipule qu'aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.
4. Les **lettres "NR"** figurant dans la colonne de droite signalent un document de priorité que le Bureau international n'a pas reçu ou que le déposant n'a pas demandé à l'office récepteur de préparer et de transmettre au Bureau international, conformément à la règle 17.1.a) ou b), respectivement. Dans ce cas, **l'attention du déposant est appelée** sur la règle 17.1.c) qui stipule qu'aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.

Date de priorité	Demande de priorité n°	Pays, office régional ou office récepteur selon le PCT	Date de réception du document de priorité
27 janv 1999 (27.01.99)	99/00887	FR	04 févr 2000 (04.02.00)

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé:

Yolaine CUSSAC

no de téléphone (41-22) 338.83.38

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

AVIS INFORMANT LE DEPOSANT DE LA COMMUNICATION DE LA DEMANDE INTERNATIONALE AUX OFFICES DESIGNES

(règle 47.1.c), première phrase, du PCT)

Destinataire:
DU BOISBAUDRY, Dominique
Société De Protection Des Inventions
3, Rue Du Docteur Lancereaux
F-75008 Paris
FRANCE

SPI - Groupe BREVATOME
14 AOUT 2000
3, rue du Docteur Lancereaux
75008 PARIS

Date d'expédition (jour/mois/année) 03 août 2000 (03.08.00)	
Référence du dossier du déposant ou du mandataire SP16207.C RS	**AVIS IMPORTANT**

Demande internationale no	**Date du dépôt international** (jour/mois/année)	**Date de priorité** (jour/mois/année)
PCT/FR00/00174	26 janvier 2000 (26.01.00)	27 janvier 1999 (27.01.99)

Déposant
FRANCE TELECOM etc

1. Il est notifié par la présente qu'à la date indiquée ci-dessus comme date d'expédition de cet avis, le Bureau international a communiqué, comme le prévoit l'article 20, la demande internationale aux offices désignés suivants:
   JP,US

   Conformément à la règle 47.1.c), troisième phrase, ces offices acceptent le présent avis comme preuve déterminante du fait que la communication de la demande internationale a bien eu lieu à la date d'expédition indiquée plus haut, et le déposant n'est pas tenu de remettre de copie de la demande internationale à l'office ou aux offices désignés.

2. Les offices désignés suivants ont renoncé à l'exigence selon laquelle cette communication doit être effectuée à cette date:
   CA,EP

   La communication sera effectuée seulement sur demande de ces offices. De plus, le déposant n'est pas tenu de remettre de copie de la demande internationale aux offices en question (règle 49.1)a-bis)).

3. Le présent avis est accompagné d'une copie de la demande internationale publiée par le Bureau international le
   03 août 2000 (03.08.00) sous le numéro WO 00/45549

RAPPEL CONCERNANT LE CHAPITRE II (article 31.2)a) et règle 54.2)

Si le déposant souhaite reporter l'ouverture de la phase nationale jusqu'à 30 mois (ou plus pour ce qui concerne certains offices) à compter de la date de priorité, **la demande d'examen préliminaire international** doit être présentée à l'administration compétente chargée de l'examen préliminaire international avant l'expiration d'un délai de 19 mois à compter de la date de priorité.

Il appartient exclusivement au déposant de veiller au respect du délai de 19 mois.

Il est à noter que seul un déposant qui est ressortissant d'un Etat contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international.

RAPPEL CONCERNANT L'OUVERTURE DE LA PHASE NATIONALE (article 22 ou 39.1))

Si le déposant souhaite que la demande internationale procède en phase nationale, il doit, dans le délai de 20 mois ou de 30 mois, ou plus pour ce qui concerne certains offices, accomplir les actes mentionnés dans ces dispositions auprès de chaque office désigné ou élu.

Pour d'autres informations importantes concernant les délais et les actes à accomplir pour l'ouverture de la phase nationale, voir l'annexe du formulaire PCT/IB/301 (Notification de la réception de l'exemplaire original) et le volume II du Guide du déposant du PCT.

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé
J. Zahra

no de téléphone (41-22) 338.83.38

TRAITE DE)OPERATION EN MATIERE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Destinataire:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 29 août 2000 (29.08.00)	
Demande internationale no PCT/FR00/00174	**Référence du dossier du déposant ou du mandataire** SP16207.C RS
Date du dépôt international (jour/mois/année) 26 janvier 2000 (26.01.00)	**Date de priorité** (jour/mois/année) 27 janvier 1999 (27.01.99)
Déposant GIRAULT, Marc etc	

1. L'office désigné est avisé de son élection qui a été faite:

[X] dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

22 juillet 2000 (22.07.00)

[ ] dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection [X] a été faite

[ ] n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé
Henrik Nyberg

no de téléphone: (41-22) 338.83.38

Copie à l'intention de l'office élu (EO/US) PCT/FR00/00174

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION DE L'ENREGISTREMENT D'UN CHANGEMENT

(règle 92bis.1 et instruction administrative 422 du PCT)

Destinataire:

DU BOISBAUDRY, Dominique
Brevalex
3, Rue Du Docteur Lancereaux
F-75008 Paris
FRANCE

Date d'expédition (jour/mois/année)
27 avril 2001 (27.04.01)

Référence du dossier du déposant ou du mandataire
SP16207.C RS

NOTIFICATION IMPORTANTE

Demande internationale no
PCT/FR00/00174

Date du dépôt international (jour/mois/année)
26 janvier 2000 (26.01.00)

1. Les renseignements suivants étaient enregistrés en ce qui concerne:

☐ le déposant ☐ l'inventeur ☒ le mandataire ☐ le représentant commun

Nom et adresse

DU BOISBAUDRY, Dominique
Société De Protection Des Inventions
3, Rue Du Docteur Lancereaux
F-75008 Paris
FRANCE

Nationalité (nom de l'Etat):

Domicile (nom de l'Etat):

no de téléphone
01 53 83 94 00

no de télécopieur
01 45 63 83 33

no de téléimprimeur

2. Le Bureau international notifie au déposant que le changement indiqué ci-après a été enregistré en ce qui concerne:

☐ la personne ☐ le nom ☒ l'adresse ☐ la nationalité ☐ le domicile

Nom et adresse

DU BOISBAUDRY, Dominique
Brevalex
3, Rue Du Docteur Lancereaux
F-75008 Paris
FRANCE

Nationalité (nom de l'Etat):

Domicile (nom de l'Etat):

no de téléphone
01 53 83 94 00

no de télécopieur
01 45 63 83 33

no de téléimprimeur

3. Observations complémentaires, le cas échéant:

4. Une copie de cette notification a été envoyée:

☒ à l'office récepteur
☐ à l'administration chargée de la recherche internationale
☐ à l'administration chargée de l'examen préliminaire international
☐ aux offices désignés concernés
☒ aux offices élus concernés
☐ autre destinataire:

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé:
Sean Taylor

no de téléphone (41-22) 338.83.38

Formulaire PCT/IB/306 (mars 1994)

003990485